



UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1460
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/072,331	02/07/2002	Philip D. MacKenzie	8-8	3140

7590 02/21/2006

Ryan, Mason & Lewis, LLP
90 Forest Avenue
Locust Valley, NY 11560

EXAMINER

BAUM, RONALD

ART UNIT PAPER NUMBER

2136

DATE MAILED: 02/21/2006

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary

Application No.

10/072,331

Applicant(s)

MACKENZIE ET AL.

Examiner

Ronald Baum

Art Unit

2136

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

- 1) ☐ Responsive to communication(s) filed on ____.
- 2a) ☐ This action is FINAL. 2b) ☒ This action is non-final.
- 3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

- 4) ☒ Claim(s) 1-34 is/are pending in the application.
- 4a) Of the above claim(s) ____ is/are withdrawn from consideration.
- 5) ☐ Claim(s) ____ is/are allowed.
- 6) ☒ Claim(s) 1-14, 16-30, 32 and 33 is/are rejected.
- 7) ☒ Claim(s) 15, 31 and 34 is/are objected to.
- 8) ☐ Claim(s) ____ are subject to restriction and/or election requirement.

Application Papers

- 9) ☐ The specification is objected to by the Examiner.
- 10) ☐ The drawing(s) filed on ____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.
Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).
Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).
- 11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

- 12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).
- a) ☐ All b) ☐ Some * c) ☐ None of:
- ☐ Certified copies of the priority documents have been received.
 - ☐ Certified copies of the priority documents have been received in Application No. ____.
 - ☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

- 1) ☒ Notice of References Cited (PTO-892)
- 2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
- 3) ☒ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
Paper No(s)/Mail Date 6/1/02
- 4) ☐ Interview Summary (PTO-413)
Paper No(s)/Mail Date. ____.
- 5) ☐ Notice of Informal Patent Application (PTO-152)
- 6) ☐ Other: ____.

DETAILED ACTION

1. Claims 1-34 are pending for examination.
2. Claims 1-14,16-30,32-33 are rejected.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claim 18 recites the limitation "*the* request to ignore" in reference to claim 14. There is insufficient antecedent basis for this limitation in the claim. For the sake of applying art, the examiner assumes the phrase should be "The method of claim 15". Correction is required.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

(b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

4. Claims 1-14,16-17, 19-30,32-33 are rejected under 35 U.S.C. 102(b) as being anticipated by Camp et al, U.S. Patent 6,317,729 B1.

5. As per claim 1; "A method for use in a device associated with a first party for performing a key retrieval operation, the method comprising the steps of:

generating in the first party device a request for

the partial assistance of a device associated with a second party in recovering

a key from

data stored on the first party device,

wherein

the second party device is remote from

the first party device [Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols applied to enabling encrypted products (i.e., enabling use of an encrypted key resident with the encrypted product that the SET is involved with) via bank verification of customer financial viability/authorization (i.e., via the bank/merchant message sequence and subsequent merchant/customer message sequence), clearly encompasses 'generating ... request ... partial assistance ... second party ... recovering ... key ... second party ... remote ... first party', as broadly interpreted by the examiner.];

transmitting the request from

the first party device to

the second party device [Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols applied to enabling encrypted products (customer to merchant purchase request, verification message sequences, delivery of decryption key for encrypted product), clearly encompasses 'transmitting the request ... first party ... second party', as broadly interpreted by the examiner.];

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device [Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols applied to enabling encrypted products (merchant to customer verification message sequences, delivery of decryption key for encrypted product), clearly encompasses 'receiving results ... first party ... second party', as broadly interpreted by the examiner.]; and

using at least a portion of the received results in the first party device to recover the key for subsequent use as

a private key in

one or more associated public key cryptographic techniques

[Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols applied to enabling encrypted (i.e., PKI, etc., SET inclusive cryptographic techniques) products (customer use of decryption key delivered for encrypted product), clearly encompasses 'using ... portion ... results ... first party ... recover the key ... public key cryptographic techniques', as broadly interpreted by the examiner.].”.

As per claim 13, this claim is the apparatus claim for the method claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection; “Apparatus for use in a device associated with a first party for performing a key retrieval operation, the apparatus comprising:

at least one processor operable to:

(i) generate in the first party device a request for

the partial assistance of a device associated with a second party in
recovering

a key from

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

(ii) transmit the request from

the first party device to

the second party device;

(iii) receive results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

(iv) use at least a portion of the received results in the first party device to

recover the key for subsequent use as

a private key in

one or more associated public key cryptographic

techniques; and

memory, coupled to the at least one processor, for storing

at least a portion of results associated with

one or more operations performed by the processor.”.

As per claim 11, this claim is the method claim for the method claim 1 above from the perspective of the server, and is rejected for the same reasons provided for the claim 1 rejection; “A method for use in a device associated with a first party for assisting in the performance of a key retrieval operation, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for

the partial assistance of the first party device in recovering

a key from

data stored on the second party device,

wherein

the first party device is remote from

the second party device; and

generating results in the first party device based on

the partial assistance provided thereby for use in the second party device to

recover the key for subsequent use as

a private key in

one or more associated public key cryptographic

techniques.”.

As per claim 14, this claim is the method claim for the method claim 1 above whereas the ‘private key operation ... public key cryptographic techniques’ in the preamble is a more specific

Art Unit: 2136

embodiment of claim 1, and is rejected for the same reasons provided for the claim 1 rejection;

“A method for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

generating in the first party device a request for

the partial assistance of a device associated with a second party in performing

a private key operation using a private key associated with

data stored on the first party device,

wherein

the second party device is remote from

the first party device;

transmitting the request from the first party device to the second party device;

receiving results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

using at least a portion of the received results in the first party device to perform the private key operation.”.

As per claim 33, this claim is the apparatus claim for the method claim 14 above, and is rejected for the same reasons provided for the claim 14 rejection; “Apparatus for use in a device associated with a first party for performing a private key operation associated with one or more public key cryptographic techniques, the apparatus comprising:

at least one processor operable to:

(i) generate in the first party device a request for

the partial assistance of a device associated with a second party in
performing

a private key operation using a private key associated with
data stored on the first party device,

wherein

the second party device is remote from

the first party device;

(ii) transmit the request from the first party device to the second party device;

(iii) receive results in the first party device generated by

the second party device based on

the partial assistance provided by the second party device; and

(iv) use at least a portion of the received results in the first party device to perform

the private key operation; and

memory, coupled to the at least one processor, for storing at least a portion of results

associated with one or more operations performed by the processor.”.

As per claim 30, this claim is the method claim for the method claim 14 above from the perspective of the server, and is rejected for the same reasons provided for the claim 14 rejection;

“A method for use in a device associated with a first party for assisting in performing a private

Art Unit: 2136

key operation associated with one or more public key cryptographic techniques, the method comprising the steps of:

receiving a request generating in and transmitted by a second party device for
the partial assistance of the first party device in performing
a private key operation using a private key associated with
data stored on the second party device,

wherein

the first party device is remote from

the second party device; and

generating results in the first party device based on

the partial assistance provided thereby for use in the second party device to
perform the private key operation.”.

6. Claim 2 *additionally recites* the limitation that; “The method of claim 1, wherein
the first party device is a client device and
the second party device is a server.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols are clearly network oriented architectures and inclusive of specifically client server networks where the customer would typically be a client network element, and, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 16, this claim is the method claim for the method claim 2 above whereas the ‘private key operation ... public key cryptographic techniques’ in the preamble is a more specific embodiment of claim 2, and is rejected for the same reasons provided for the claim 2 rejection;

“The method of claim 14, wherein

the first party device is a client device and

the second party device is a server.”.

As per claim 12, this claim is the method claim for the method claim 2 above from the perspective of the server, such that the ‘first party device’, ‘second party device’, designations in the claim language are reversed, and is rejected for the same reasons provided for the claim 2 rejection; “The method of claim 11, wherein

the first party device is a server and

the second party device is a client device.”.

As per claim 32, this claim is the method claim for the method claim 16 above from the perspective of the server, and is rejected for the same reasons provided for the claim 16 rejection;

“The method of claim 30, wherein

the first party device is a server and

the second party device is a client device.”.

7. Claim 3 *additionally recites* the limitation that; “The method of claim 1, wherein
the data stored on the first party device has

a piece of secret information associated therewith which
is included in the request, and further wherein
the partial assistance is provided by the second party device when
a verification is made by the second party device,
based on the piece of secret information,
that the first party sent the request”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer identification and financial information, clearly secret, to merchant to bank verification message sequences, clearly partial assistance, delivery of decryption key for encrypted product), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 17, this claim is the method claim for the method claim 3 above whereas the ‘private key operation ... public key cryptographic techniques’ in the preamble is a more specific embodiment of claim 3, and is rejected for the same reasons provided for the claim 3 rejection; “The method of claim 14, wherein

the data stored on the first party device has
a piece of secret information associated therewith which
is included in the request, and further wherein
the partial assistance is provided by the second party device when
a verification is made by the second party device,

based on the piece of secret information,
that the first party sent the request.”.

8. Claim 4 ***additionally recites*** the limitation that; “The method of claim 1, wherein the request generated by the first party device comprises
cryptographic information
included in the data stored on the first party device and
previously generated from the key.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer identification and financial information, HASHed and clearly cryptographic information, to merchant to bank verification message sequences, clearly partial assistance, delivery of decryption key for encrypted product (i.e., enabling use of an encrypted key resident with the encrypted product that the SET is involved with)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

9. Claim 5 ***additionally recites*** the limitation that; “The method of claim 4, wherein the cryptographic information is generated via
an encryption operation which is a function of
one or more pieces of secret information associated with the first party,
the key, and
a public key associated with the second party device.”.

Art Unit: 2136

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer information, HASHed encryption operation of cryptographic information, to merchant to bank verification message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

10. Claim 6 *additionally recites* the limitation that; “The method of claim 4, wherein the results generated by the second party device comprise
- results associated with the second party device partially decrypting
- at least a portion of the cryptographic information in the request.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer information, processed HASHed encryption operation of cryptographic information and resulting bank verification message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

11. Claim 7 *additionally recites* the limitation that; “The method of claim 6, wherein the step of using at least a portion of the received results in the first party device further comprises
- completing the decryption of
- at least a portion of the cryptographic information to

recover the key.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer information, processed HASHed encryption operation of cryptographic information and resulting bank verification message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

12. Claim 8 *additionally recites* the limitation that; “The method of claim 1, further comprising

the step of at least temporarily storing the recovered key at the first party device.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols and associated request/response information is clearly stored as both persistent and non-persistent (i.e., temporarily) data at the various network nodes, clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

13. Claim 9 *additionally recites* the limitation that; “The method of claim 1, wherein the one or more associated public key cryptographic techniques comprise

decryption or

signature operations.”.

Art Unit: 2136

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (secure challenge/response, signing, authorization/authentication sequences, content/message encryption/decryption, etc.), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

14. Claim 10 *additionally recites* the limitation that; “The method of claim 1, wherein
no pre-registration process need take place between
the first party device and
the second party device.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols are communicated over the Internet (i.e., ad-hoc and therefore a non pre-registration process at the higher OSI layers), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

As per claim 29, this claim is the method claim for the method claim 10 above whereas the ‘private key operation ... public key cryptographic techniques’ in the preamble is a more specific embodiment of claim 10, and is rejected for the same reasons provided for the claim 10 rejection; “The method of claim 14, wherein

no pre-registration process need take place between
the first party device and

the second party device.”.

15. Claim 19 *additionally recites* the limitation that; “The method of claim 14, wherein the step of sharing the performance of the private key operation comprises a function sharing operation.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (secure challenge/response, signing, authorization/authentication sequences, content/message encryption/decryption and associated function sharing, etc.), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

16. Claim 20 *additionally recites* the limitation that; “The method of claim 14, wherein the data stored on the first party device was constructed by generating a first share and a second share of a private key associated with the first party device.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (secure challenge/response, transaction batching and associated partial/full rollback, signing, authorization/authentication sequences, content/message encryption/decryption and associated function sharing, etc.), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

17. Claim 21 *additionally recites* the limitation that; “The method of claim 20, wherein the first share is constructed so that the share can be generated from a piece of secret information associated with the first party and information stored on the first party device.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer identification and financial information, clearly secret, to merchant to bank verification message sequences, secure challenge/response, transaction batching and associated partial/full rollback, signing, authorization/authentication sequences, content/message encryption/decryption and associated function sharing, etc.), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

18. Claim 22 *additionally recites* the limitation that; “The method of claim 21, wherein the data stored on the first party device comprises an encryption of at least the second share of the private key in accordance with a public key associated with the second party device so as to generate cryptographic information.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (transaction batching and associated partial/full rollback, signing,

authorization/authentication sequences, content/message encryption/decryption and associated function sharing, of which in the sharing case, partial (i.e., granularity aspects per se) and full encryption/private key functionality is enabled, etc.), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

19. Claim 23 *additionally recites* the limitation that; “The method of claim 21, wherein the request generated in the first party device comprises the cryptographic information.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (secure challenge/response, signing/authorization/authentication sequences (i.e., cryptographic information), content/message encryption/decryption, etc.), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

20. Claim 24 *additionally recites* the limitation that; “The method of claim 23, wherein the step of using at least a portion of the received results in the first party device to perform the private key operation comprises

completing a computation of the private key operation at the first party device using results of a computation portion contributed by the second party device.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (customer information, processed HASHed encryption operation of

Art Unit: 2136

cryptographic information and resulting bank verification message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

21. Claim 25 *additionally recites* the limitation that; “The method of claim 14, wherein the private key operation comprises a decryption operation.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (processed HASHed encryption operation of cryptographic information and resulting bank verification (i.e., decryption aspects) message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

22. Claim 26 *additionally recites* the limitation that; “The method of claim 25, wherein the decryption operation comprises an ElGamal protocol.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (processed HASHed encryption operation of cryptographic information and resulting bank verification (i.e., ElGamal decryption/key transfer aspects) message sequences

Art Unit: 2136

(inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

23. Claim 27 *additionally recites* the limitation that; “The method of claim 14, wherein the private key operation comprises
a signature operation.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (processed HASHed encryption operation of cryptographic information and resulting bank verification (i.e., signature operation aspects) message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

24. Claim 28 *additionally recites* the limitation that; “The method of claim 27, wherein the signature operation comprises
an RSA protocol.”.

The teachings of Camp et al are directed towards such limitations (i.e., Abstract, figures 1-2 and accompanying descriptions with figure 2 more particularly, whereas the SET standardized secure transaction protocols (processed HASHed encryption operation of cryptographic information and resulting bank verification (i.e., signature operation RSA protocol aspects) message sequences (inclusive of cross authentication which deals with the second device public key)), clearly encompasses the claim limitations, as broadly interpreted by the examiner.).

Allowable Subject Matter

25. Claims 15, 18, 31 and 34 are objected to as being dependent upon a rejected base claim, but would be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims.

Art Unit: 2136

Conclusion


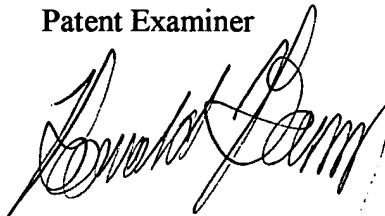
26. Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (571) 272-3861, and whose unofficial Fax number is (571) 273-3861. The examiner can normally be reached Monday through Thursday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (571) 272-3795. The Fax number for the organization where this application is assigned is **571-273-8300**.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. For more information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see <http://pair-direct.uspto.gov>. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

Ronald Baum

Patent Examiner



AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100